中信國際電訊CPC
CITIC TELECOM CPC

TrustCSI™ UTM 統一威脅管理

備有智能綜合警報的網絡安全管理方案

互聯網全面開放，加上現代商業活動複雜，企業內部與外部又高密互連，結合種種因素，形成對企業造成廣泛的安全風險，包括源自公司外部或內部的黑客、安全威脅以及網絡漏洞。

許多企業都已應用防火牆及虛擬專用網絡(VPN)作為他們抵擋惡意攻擊的第一度防禦，可惜這只能對已知的威脅維持最低限度的保護，卻不能阻截新興的非蓄意內部威脅對企業網絡的攻擊。

中信國際電訊CPC的 **TrustCSI™ UTM** 統一威脅管理方案為企業提供無憂式第一線網絡防禦，既不用硬件投資，將技術支援負擔降至最低，卻能更全面保護機構的資訊安全。

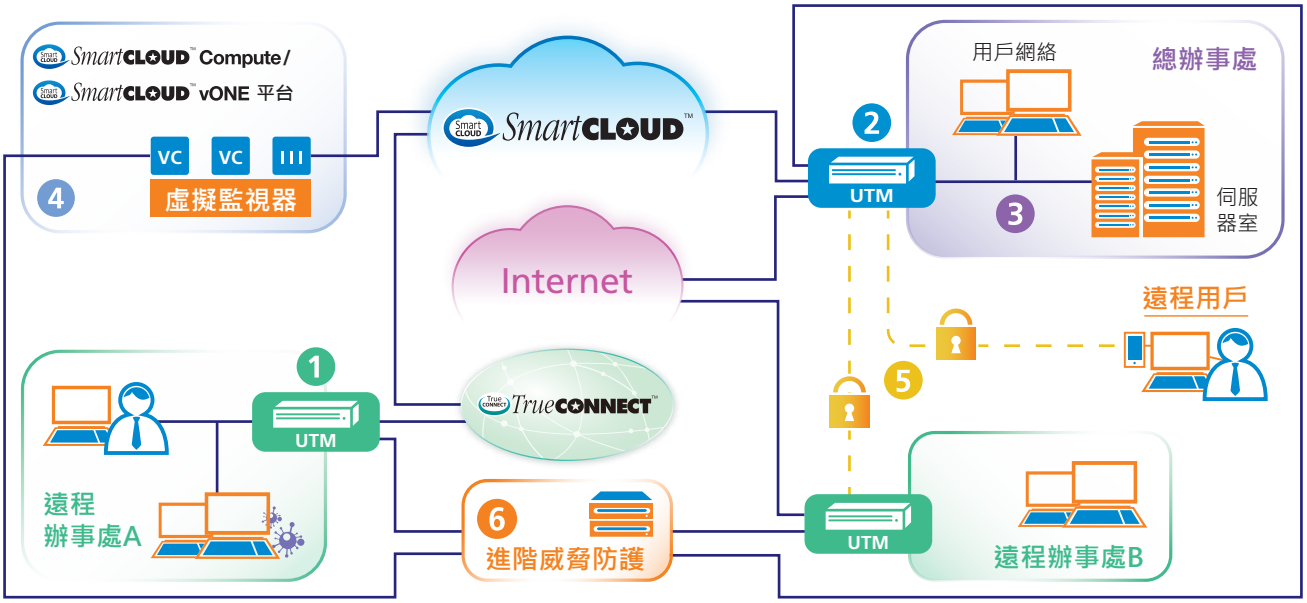
產品特點

- 安全專家全面管理，提供24 x 7實時監察、現場支援及熱線服務，另設綜合警報電郵及利用SIEM技術平台作關聯分析
- 多合一功能，包括防火牆、防病毒、防垃圾電郵、入侵防護系統(IPS)以及網上活動管制
- 用戶的實時監察網站及每週的安全管理報告
- 客戶可選擇由SmartCLOUD™基建支援的TrustCSI™ UTM NFV軟件型虛擬設備，並享有99.99%的高可用性服務
- 客戶可選擇 TrustCSI™ Managed YourDevice服務由我們專業人員為你的安全設備提供遠程監控和管理服務
- 靈活的月費模式及系統更新，可按業務的安全需要而擴展
- 器材配置管理、備份及預先更換硬件裝置服務
- 備有IPSec VPN，SSL VPN及廣域網絡優化功能
- SmartCLOUD™用戶可選擇TrustCSI™ UTM NFV軟件型虛擬設備，相比傳統硬件型的統一威脅管理方案，可縮短服務開通時間

你最可信賴的信息技術方案伙伴

TrustCSI™ UTM 統一威脅管理

企業網絡的多層保護措施



1. MPLS層次的跨地區病毒傳播保護及用戶認證功能

參閱附圖，TrustCSI™ UTM統一威脅管理方案可防止企業MPLS網絡內的威脅，阻隔遠程辦事處A的病毒散播至其他辦事處，即遠程辦事處B和公司總部。另外，用戶認證功能可為企業的關鍵資產提供進一步的存取控制。圖中只有用戶C，通過企業指定的用戶認證規定，如“電子証書”，方可存取伺服器的關鍵資料。

2. 互聯網層次的閘道保護

為了避免安全威脅透過如員工上網瀏覽等活動，經由互聯網入侵公司網絡，TrustCSI™ UTM統一威脅管理方案可有效保護資料透過在互聯網上的不信任區域傳送。

3. 關鍵資產保護

TrustCSI™ UTM統一威脅管理方案可提供不同部署模式，把企業網絡分隔成不同區域，妥善保障較為容易受到攻擊，而後果極為嚴重的企業關鍵資產，免受內部和外部的威脅，包括：設置於企業內，供員工經常存取的檔案伺服器，及與互聯網連接的伺服器。

4. 虛擬安全閘道連接SmartCLOUD™平台

為保護部署在SmartCLOUD™ Compute和vONE雲平台上的基建，企業可彈性及快速地部署虛擬化TrustCSI™ UTM統一威脅管理方案。

5. 彈性VPN部署確保安全遠程存取

企業網絡可通過互聯網，並透過IPSec加密管道，延伸至遠程辦事處B。遠程用戶亦可利用流動裝置，透過SSL VPN管道取得內部資源(檔案伺服器，業務應用程式)。

6. 抵禦進階持續性威脅

TrustCSI™ UTM統一威脅方案可與沙盒或雲端沙盒服務協作及連繫以防禦日益嚴重的進階持續性威脅。當附有惡意程式或可疑檔案一被識別，沙盒將發送警報至TrustCSI™ UTM統一威脅管理作自動回應或消除威脅。

中信國際電訊CPC

W: www.citictel-cpc.com
亞太區: info@citictel-cpc.com
歐洲及CIS: info-eu@citictel-cpc.com

香港 T: 852 2170 7101
日本 T: 81 3 5339 1968
愛沙尼亞 T: 372 622 33 99
俄羅斯 T: 7 495 981 5676
台灣 T: 886 2 6600 2588
馬來西亞 T: 603 2280 1500
波蘭 T: 48 22 630 63 30
荷蘭 T: 31 20 567 2000
中國大陸 (Toll Free): 400 651 7550
新加坡 T: 65 6220 6606

TUM1909EN